Inventor: Docket No.:

1/14



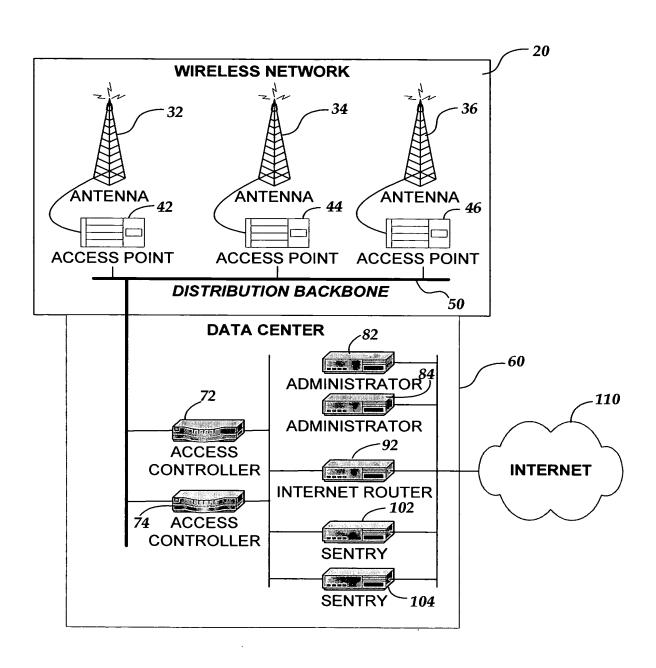
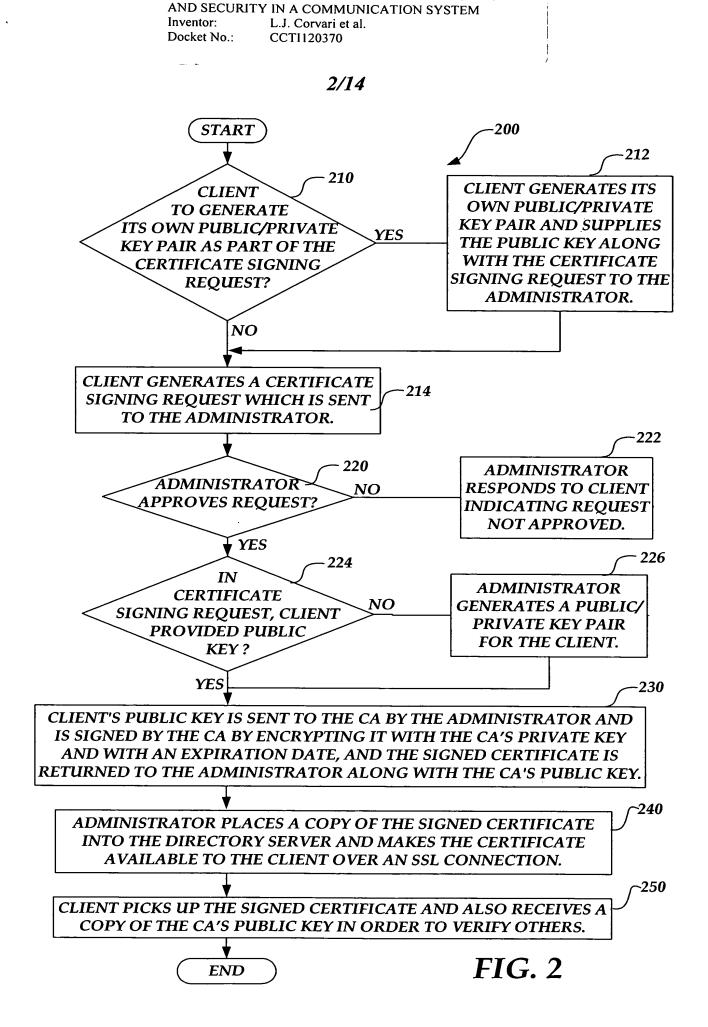


FIG. 1



Title: SYSTEM AND METHOD FOR AUTHENTICATION

Inventor: Docket No.:

3/14

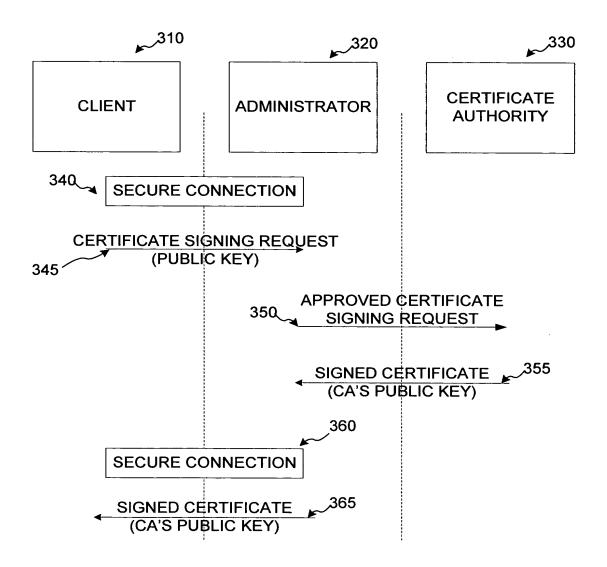


FIG. 3A

Inventor: L.J. Corvari et al. Docket No.: CCT1120370

4/14

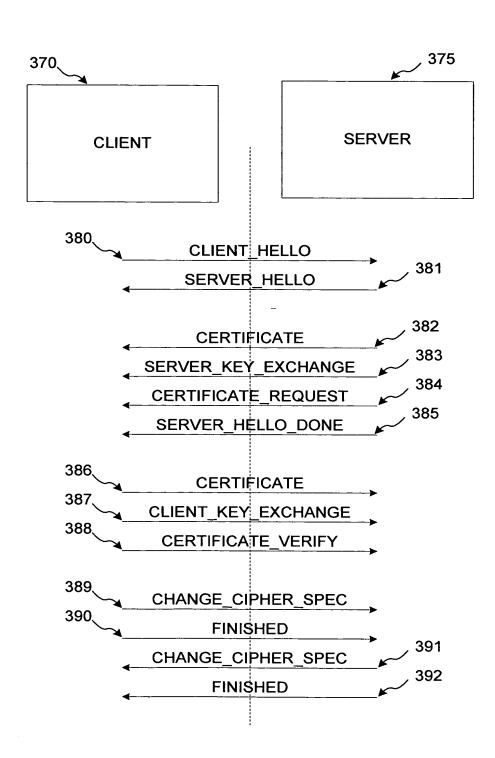
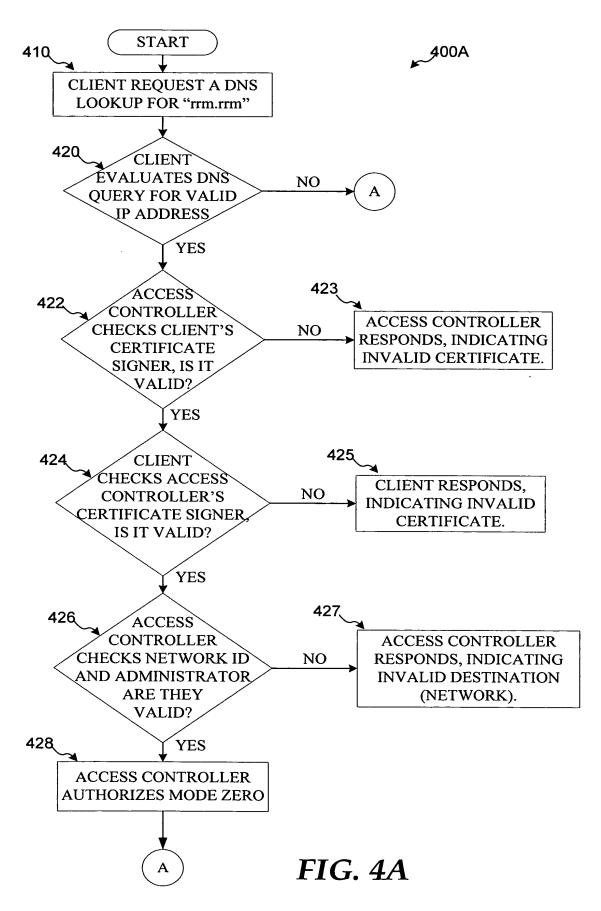


FIG. 3B

Title: SYSTEM AND METHOD FOR AUTHENTICATION AND SECURITY IN A COMMUNICATION SYSTEM Inventor: L.J. Corvari et al.

Inventor:
Docket No.:

5/14



Inventor: L.J. Corvari et al. Docket No.: CCTI120370 6/14 400B 430 CLIENT SENDS REGISTRATION MESSAGE TO ADMINISTRATOR WITH A SIGNED PUBLIC KEY IN THE CLEAR AND A DIGITALLY SIGNED MESSAGE DIGEST ENCRYPTED WITH THE CLIENT'S PRIVATE KEY 440 **ADMINISTRATOR DECRYPTS DIGITAL** SIGNATURE WITH CLIENT'S PUBLIC ADMINISTRATOR NO KEY AND RECALCULATES MESSAGE RESPONDS, INDICATING DIGEST AND COMPARES AND TAMPERING. THEREBY VERIFIES NO TAMPERING? YES 443 **ADMINISTRATOR** ADMINISTRATOR CHECKS THE SIGNING NO RESPONDS, INDICATING CERTIFICATE AUTHORITY, IS IT NON TRUSTED TRUSTED? CERTIFICATE AUTHORITY YES 445 **ADMINISTRATOR ADMINISTRATOR** NO VERIFIES THE EXPIRATION DATE RESPONDS, INDICATING IN THE CLIENT'S SIGNED PAST EXPIRATION DATE. PUBLIC KEY YES 447 446 ADMINISTRATOR ADMINISTRATOR CHECKS THE USER ID NO. RESPONDS, INDICATING EITHER THE USER ID OR AND PASSWORD, ARE THEY PASSWORD ARE INVALID. VALID? YES 449 **ADMINISTRATOR** ADMINISTRATOR RESPONDS, INDICATING VERIFIES THE SIGNED NO THAT THE PUBLIC KEY IS PUBLIC KEY IS IN THE DIRECTORY NOT IN THE DIRECTORY SERVER AND HAS NOT BEEN SERVER OR HAS BEEN **REVOKED?** REVOKED. YES FIG. 4B

Title: SYSTEM AND METHOD FOR AUTHENTICATION AND SECURITY IN A COMMUNICATION SYSTEM

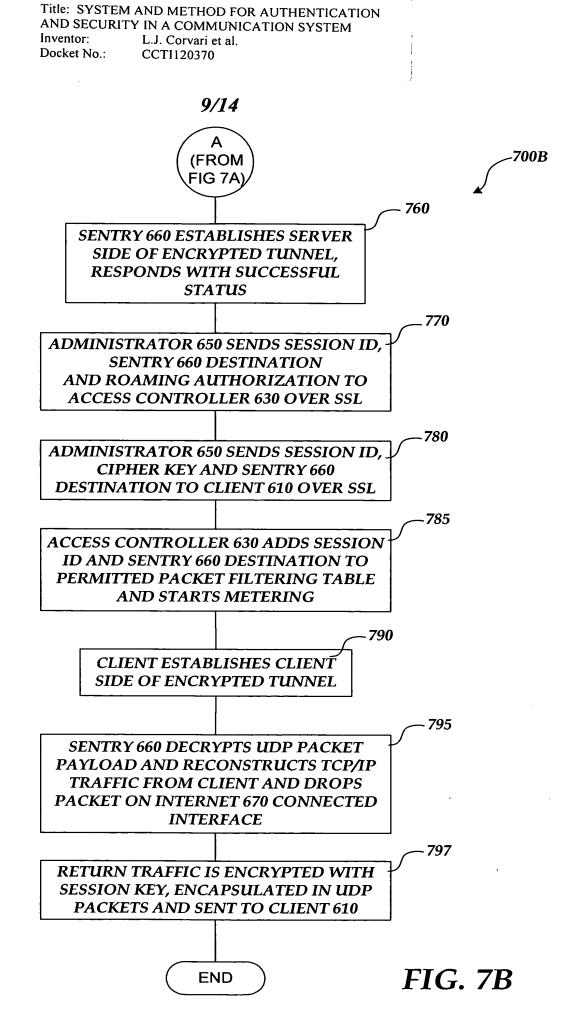
Inventor: L.J. Corvari et al. Docket No.: CCTI120370 7/14 _400C 450 ADMINISTRATOR RANDOMLY GENERATES BOTH A SESSION ID AND A NEW SESSION KEY FOR USE WITH SYMMETRICAL ENCRYPTION FOR ONE-TIME USE (FOR THE DURATION OF THE SESSION) AND A COPY OF THE ADMINISTRATOR'S SIGNED PUBLIC KEY. 452 ADMINISTRATOR SENDS BOTH THE SESSION ID AND THE SESSION KEY TO THE SENTRY OVER A SECURE CONNECTION. 454 SENTRY SENDS THE CLIENT VIRTUAL IP ADDRESS TO THE ADMINISTRATOR OVER A SECURE CONNECTION 456 ADMINISTRATOR SEND A NETWORK ACCESS AUTHORIZATION MESSAGE TO THE ACCESS CONTROLLER OVER A SECURE CONNECTION **458**\ THE MESSAGE INCLUDING THE SESSION ID, THE SESSION KEY, AND VIRTUAL IP IS ENCRYPTED WITH THE CLIENT'S PUBLIC KEY AND INCLUDES A DIGITAL SIGNATURE WITH A MESSAGE DIGEST ENCRYPTED BY THE ADMINISTRATOR'S SIGNED PRIVATE KEY. **460** ADMINISTRATOR SENDS THE SESSION ID, SESSION KEY, CLIENT VIRTUAL IP ADDRESS, AND ADDRESS OF THE SENTRY TO THE CLIENT. 470 NEW SESSION KEY IS USED TO ENCRYPT ALL FURTHER NETWORK TRAFFIC FOR THE DURATION OF THE CURRENT SESSION. 480 THE CLIENT VIRTUAL IP IS USED AS THE SOURCE FOR ALL IP PACKETS WHICH ARE ENCAPSULATED INTO AN IP PACKET DESTINED FOR THE SENTRY **END**

Title: SYSTEM AND METHOD FOR AUTHENTICATION AND SECURITY IN A COMMUNICATION SYSTEM

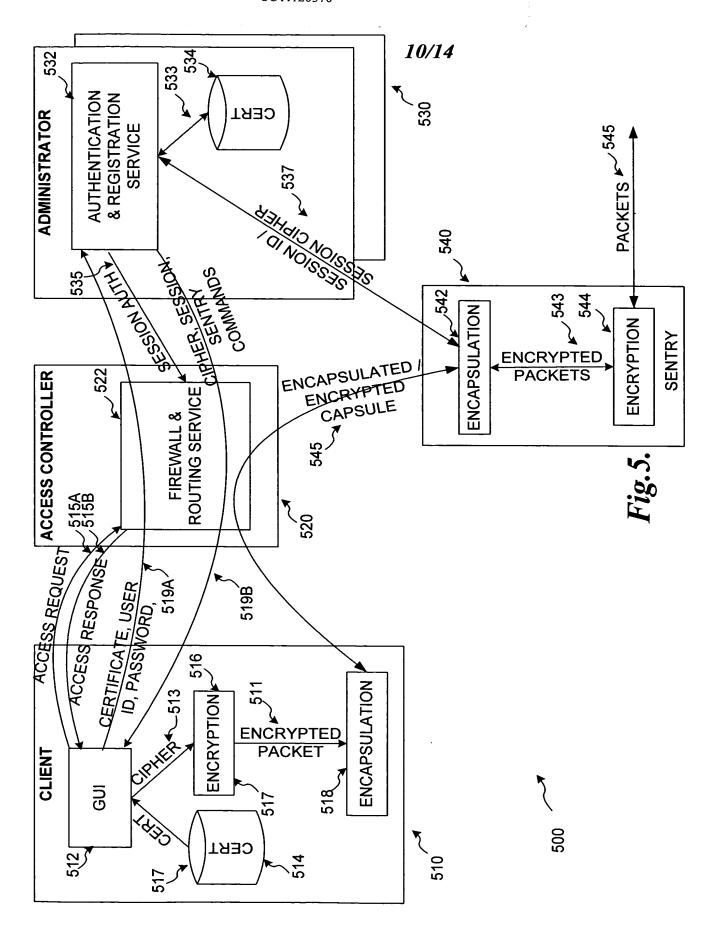
FIG. 4C

Inventor: L.J. Corvari et al. Docket No.: CCTI120370 8/14 **START** -700A 710 **CLIENT 610 LOOKS UP ACCESS CONTROLLER 630 ADDRESS** 720 **CLIENT 610 MAKES A SECURE** CONNECTION TO ACCESS CONTROLLER 630 AND IDENTIFIES ITSELF AS A MEMBER OF "NETWORK B" AND INCLUDES HOME ADMINISTRATOR 650 ADDRESS 730 **ACCESS CONTROLLER 630 RECOGNIZES** SIGNED CERTIFICATE AND VALIDATES ROAMING AGREEMENT WITH "NETWORK B" AND RETURNS SESSION ID X FOR TEMPORARY MODE 0 PROXY TUNNEL 740 CLIENT ENCAPSULATES IN MODE 0 TUNNEL TO ACCESS CONTROLLER 630 SSL PACKETS FOR ADMINISTRATOR 650 TO REQUEST A SECURE SESSION AND INCLUDES ACCESS **CONTROLLER 630 HOST SIDE ADDRESS** 750 ACCESS CONTROLLER 630 VALIDATES SESSION ID Y AND DESTINATION AND SENDS PACKETS THROUGH *755* ADMINISTRATOR 650 AUTHENTICATES CERTIFICATE, LOGIN/PASSWORD AND ROAMING PRIVILEGES, GENERATES SESSION ID AND SESSION KEY AND PROVISIONS ENCRYPTED TUNNEL ON SENTRY 660 A (TO FIG 7B) FIG. 7A

Title: SYSTEM AND METHOD FOR AUTHENTICATION AND SECURITY IN A COMMUNICATION SYSTEM



Inventor:
Docket No.:



Inventor: Docket No.:

009

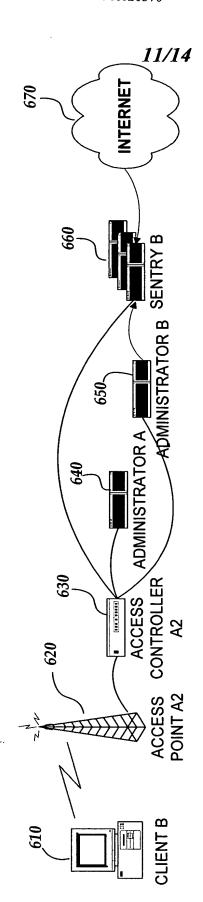


Fig.6.

Inventor: Docket No.:

12/14

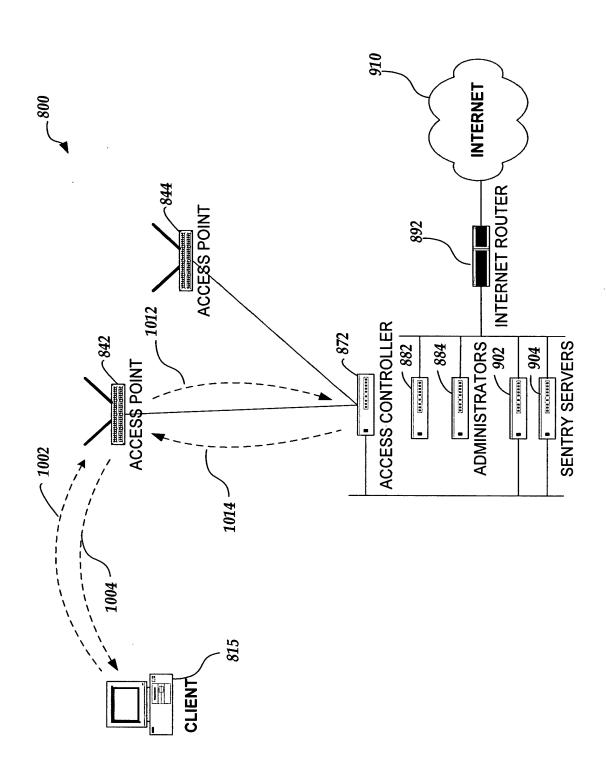
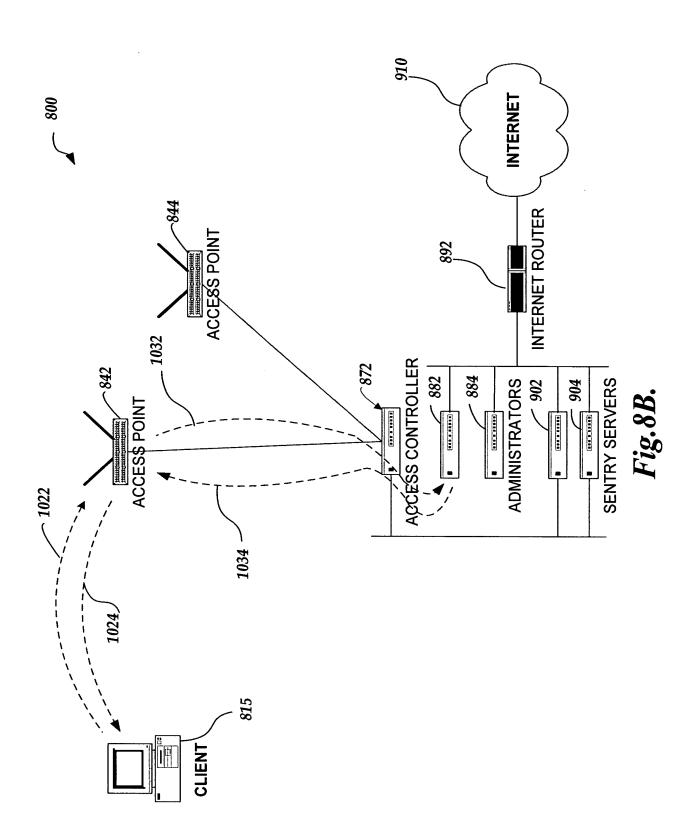


Fig. 84.

Inventor: Docket No.:

13/14



Inventor:
Docket No.:

14/14

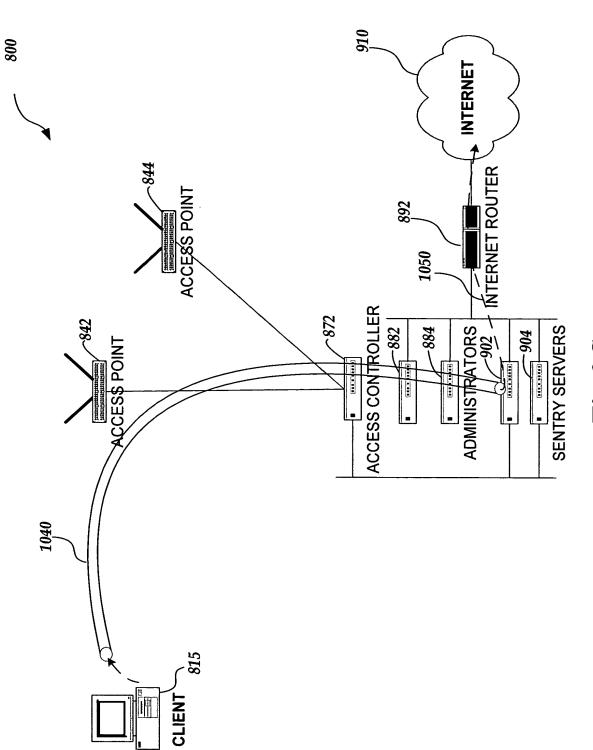


Fig.8C.